INTERFERENC SEARCH

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	(digital signature error verfication header identifier public key certificate map).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:44
S2	0	(digital signature error verfication header identifier certificate map).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:44
S3	0	(digital signature error header identifier certificate map).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:44
S4	1	(digital error header identifier certificate map).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:45
S5	1	(error header identifier certificate map).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:45
S6	4	(error header identifier certificate digital signature).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:46
S7	4	(error header identifier certificate digital signature key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:46
S8	2	(error header identifier certificate digital signature message).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:46

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1836492	(JUST, MICHAEL K).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 18:58
S2	1	(JUST, MICHAEL K).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 18:59
S3	51	(JUST, MICHAEL).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:07
S4	1	S3 and (digital adj signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/12/19 20:09
S5	0	(71/176).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/19 20:09
S6	2666	(713/176).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/19 20:09
S7	1598	S6 and @ad<"20030327"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:21
S8	0	(digital adj signature) same error same (table or map or chart) same header same (public adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:20
S10	45	(digital adj signature) same error same header same (public adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:21

EAST Search History

S11	5	S10 and @ad<"20030327"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:23
S12	9	(digital adj signature) same unauthorized same header same (public adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:23
S13	3	S12 and @ad<"20030327"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:25
S14	269	(digital adj signature) same (verif$7 or authenticat$5 or valid$7) same header same (public adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:25
S15	113	S14 and @ad<"20030327"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:39
S16	67	(digital adj signature) same fail$5 same header same (public adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:39
S17	22	S16 and @ad<"20030327"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:41
S18	66	(digital adj signature) same error same updat$6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:41
S19	24	S18 and @ad<"20030327"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/19 20:43

EAST Search History

S20	95	receiv$3 same header same certificate same (public adj key)	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/12/19 20:42

S21	8	receiv$3 same header same certificate same (public adj key) same (digital adj signature)	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/12/19 20:43

S22	4	S21 and @ad<"20030327"	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/12/19 20:43

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

"digital signature" and header and identifier and "public key" a SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used: digital signature and header and identifier and public key and certificate and acceptable and message and verification and map

Found **10,911** of **216,412**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □ ▄ ▄ ▄ ■

1 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB)

Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 A semantics for web services authentication

Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon

January 2004 **ACM SIGPLAN Notices , Proceedings of the 31st ACM SIGPLAN-SIGACT symposium on Principles of programming languages POPL '04**, Volume 39 Issue 1

Publisher: ACM Press

Full text available: pdf(234.06 KB)

Additional Information: full citation, abstract, references, citings, index terms

We consider the problem of specifying and verifying cryptographic security protocols for XML web services. The security specification WS-Security describes a range of XML security tokens, such as username tokens, public-key certificates, and digital signature blocks, amounting to a flexible vocabulary for expressing protocols. To describe the syntax of these tokens, we extend the usual XML data model with symbolic representations of cryptographic values. We use predicates on this data model to d ...

Keywords: XML security, applied pi calculus, web services

3 Applications of formal methods: Verifying policy-based security for web services

Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press
Full text available: pdf(269.16 KB) Additional Information: full citation, abstract, references, citings, index terms

WS-SecurityPolicy is a declarative configuration language for driving web services security mechanisms. We describe a formal semantics for WS-SecurityPolicy, and propose a more abstract link language for specifying the security goals of web services and their clients. Hence, we present the architecture and implementation of fully automatic tools that (1) compile policy files from link specifications, and (2) verify by invoking a theorem prover whether a set of policy files run by any number o ...

Keywords: XML security, pi calculus, web services

4 Authentication in distributed systems: theory and practice
Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4
Publisher: ACM Press
Full text available: pdf(3.37 MB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribution, loading programs, path name, principal, role, secure channel, speaks for, trusted computing base

5 A security architecture for fault-tolerant systems
Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

6 Smart packets: applying active networks to network management
Beverly Schwartz, Alden W. Jackson, W. Timothy Strayer, Wenyi Zhou, R. Dennis Rockwell, Craig Partridge
February 2000 **ACM Transactions on Computer Systems (TOCS)**, Volume 18 Issue 1

Publisher: ACM Press

Full text available: pdf(190.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This article introduces Smart Packets and describes the smart Packets architecture, the packet formats, the language and its design goals, and security considerations. Smart Packets is an Active Networks project focusing on applying active networks technology to network management and monitoring. Messages in active networks are programs that are executed at nodes on the path to one or more target hosts. Smart Packets programs are written in a tightly encoded, safe language specifically des ...

Keywords: active networks

7 Privacy enhanced mail design and implementation perspectives

D. F. Hadj Sadok, Judith Kelner

July 1994 **ACM SIGCOMM Computer Communication Review**, Volume 24 Issue 3

Publisher: ACM Press

Full text available: pdf(792.71 KB) Additional Information: full citation, abstract, index terms

The introduction of public key crypto-systems has opened the way to using security in distributed applications without imposing huge management overhead. Electronic mail is one area where security is important. Privacy Enhanced Mail is emerging as a de-facto international standard for the interchange of secure e-mail.This paper discusses some of the current problematic issues of PEM and introduces a PEM User Agent developed to test some of its concepts. A number of PEM design and implementation ...

8 Secure sessions for Web services

Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon

May 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 2

Publisher: ACM Press

Full text available: pdf(579.98 KB) Additional Information: full citation, abstract, references, index terms

We address the problem of securing sequences of SOAP messages exchanged between web services and their clients. The WS-Security standard defines basic mechanisms to secure SOAP traffic, one message at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; moreover, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-S ...

Keywords: Web services, XML security

9 FIRE: flexible Intra-AS routing environment

Craig Partridge, Alex C. Snoeren, W. Timothy Strayer, Beverly Schwartz, Matthew Condell, Isidro Castiñeyra

August 2000 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication SIGCOMM '00**, Volume 30 Issue 4

Publisher: ACM Press

Full text available: pdf(107.75 KB) Additional Information: full citation, abstract, references, citings, index terms

Current routing protocols are monolithic, specifying the algorithm used to construct forwarding tables, the metric used by the algorithm (generally some form of hop-count), and the protocol used to distribute these metrics as an integrated package. The Flexible Intra-AS Routing Environment (FIRE) is a link-state, intra-domain routing protocol that decouples these components. FIRE supports run-time-pro- grammable algorithms and metrics over a secure link-state distribution protocol. By allow ...

10 Crypto-based identifiers (CBIDs): Concepts and applications
Gabriel Montenegro, Claude Castelluccia
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

11 Web services: An advisor for web services security policies
Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, Greg O'Shea
November 2005 **Proceedings of the 2005 workshop on Secure web services SWS '05**
Publisher: ACM Press
Full text available: pdf(314.81 KB) Additional Information: full citation, abstract, references, index terms

We identify common security vulnerabilities found during security reviews of web services with policy-driven security. We describe the design of an advisor for web services security configurations, the first tool both to identify such vulnerabilities automatically and to offer redial advice. We report on its implentation as a plugin for Microsoft Web Services Enhancents (WSE).

Keywords: WS-security, XML security, policy-driven security, web services

12 Secure sessions for web services
Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon
October 2004 **Proceedings of the 2004 workshop on Secure web service SWS '04**
Publisher: ACM Press
Full text available: pdf(351.35 KB) Additional Information: full citation, abstract, references, citings

WS-Security provides basic means to secure SOAP traffic, one envelope at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; besides, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-SecureConversation introduces *security contexts*, which can be used to secure sessions between two parties. WS-Trust specifies ...

13 Role-based access control on the web
Joon S. Park, Ravi Sandhu, Gail-Joon Ahn
February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 1
Publisher: ACM Press
Full text available: pdf(331.03 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Current approaches to access control on the Web servers do not scale to enterprise-wide systems because they are mostly based on individual user identities. Hence we were motivated by the need to manage and enforce the strong and efficient RBAC access control technology in large-scale Web environments. To satisfy this requirement, we identify two different architectures for RBAC on the Web, called user-pull and server-pull. To demonstrate feasibility, we im ...

Keywords: WWW security, cookies, digital certificates, role-based access control

14 A public-key based secure mobile IP
John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

15 A secure incentive protocol for mobile ad hoc networks
Yanchao Zhang, Wenjing Lou, Wei Liu, Yuguang Fang
October 2007 **Wireless Networks**, Volume 13 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(475.04 KB) Additional Information: full citation, abstract, references, index terms

The proper functioning of mobile ad hoc networks depends on the hypothesis that each individual node is ready to forward packets for others. This common assumption, however, might be undermined by the existence of selfish users who are reluctant to act as packet relays in order to save their own resources. Such non-cooperative behavior would cause the sharp degradation of network throughput. To address this problem, we propose a credit-based Secure Incentive Protocol (SIP) to stimulate cooper ...

Keywords: cooperation, incentive, mobile ad hoc networks, security, selfishness

16 Encryption and Secure Computer Networks
Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

17 Multi-agent systems and social behavior: A user-centric anonymous authorisation framework in e-commerce environment
Richard Au, Harikrishna Vasanta, Kim-Kwang Raymond Choo, Mark Looi
March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**
Publisher: ACM Press
Full text available: pdf(291.06 KB) Additional Information: full citation, abstract, references, citings

A novel user-centric authorisation framework suitable for e-commerce in an open environment is proposed. The credential-based approach allows a user to gain access rights anonymously from various service providers who may not have pre-existing relationships. Trust establishment is achieved by making use of referrals from external third parties in the form of *Anonymous Attribute Certificates.* The concepts of *One-task*

Authorisation Key and *Binding Signature* are proposed to fac ...

18 Service-oriented device communications using the *devices profile for web services*
François Jammes, Antoine Mensch, Harm Smit
November 2005 **Proceedings of the 3rd international workshop on Middleware for pervasive and ad-hoc computing MPAC '05**
Publisher: ACM Press
Full text available: pdf(479.82 KB) Additional Information: full citation, abstract, references, index terms

This paper outlines the benefits of adopting service-oriented architectures at the level of communications between resource-constrained embedded devices. It focuses on the usage of the *Devices Profile for Web Services* as the underpinning of such architectures for "smart" devices and discusses an early implementation thereof. It further illustrates how "dumb" or "legacy" devices can be integrated using a gatewaying approach.

Keywords: communication infrastructure, device networking, service-oriented architecture, web service

19 Emerging applications: Defending against redirect attacks in mobile IP
Robert H. Deng, Jianying Zhou, Feng Bao
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**
Publisher: ACM Press
Full text available: pdf(266.04 KB) Additional Information: full citation, abstract, references, citings, index terms

The route optimization operation in Mobile IP Version 6 (MIPv6) allows direct routing from any correspondent node to any mobile node and thus eliminates the problem of "triangle routing" present in the base Mobile IP Version 4 (MIPv4) protocol. Route optimization, however, requires that a mobile node constantly inform its correspondent nodes about its new care-of addresses by sending them binding update messages. Unauthenticated or malicious binding updates open the door for intruders to perform ...

Keywords: authenticated key-exchange, mobile IP, mobile IP security, redirect attack, secure binding update

20 Authentication in distributed systems: theory and practice
Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth ACM symposium on Operating systems principles SOSP '91**, Volume 25 Issue 5
Publisher: ACM Press
Full text available: pdf(2.33 MB) Additional Information: full citation, abstract, references, citings, index terms

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegation of authority. The theory explains how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We use the th ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next